# 日本国特許庁
# JAPAN PATENT OFFICE

26.07.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　６月２０日

出願番号
Application Number: 特願２００３－１７６５６８

[ST. 10/C]: [ＪＰ２００３－１７６５６８]

出願人
Applicant(s): 日本電信電話株式会社



２００４年　９月　２日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００４－３０７８６６９

【書類名】　特許願
【整理番号】　NTTH155517
【あて先】　特許庁長官殿
【国際特許分類】　H04L 12/00
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　小野　久美子
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　立元　慎也
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　坂谷　精一
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100077274
　【弁理士】
　【氏名又は名称】　磯村　雅俊
　【電話番号】　03-3348-5035
【選任した代理人】
　【識別番号】　100102587
　【弁理士】
　【氏名又は名称】　渡邉　昌幸
　【電話番号】　03-3348-5035

【手数料の表示】

【予納台帳番号】　013402

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9701395

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セッション制御サーバ、通信装置、通信システムおよび通信方法、ならびにそのプログラムと記録媒体

【特許請求の範囲】

【請求項１】　ネットワークを介してセッション制御サーバと通信可能に接続され、１以上の前記セッション制御サーバを経由した他の通信装置との間で信号送受信を行うことで、該通信装置とのセッションを確立する通信装置において、

送信信号の守秘性を保持するために暗号化した情報を送信する際に、情報暗号化のための第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した第一の暗号化鍵を添付した、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

前記暗号化鍵暗号化手段は、該第一の暗号化鍵を、送信先の通信装置または１以上の該セッション制御サーバの各々が保有する第二の暗号化鍵を用いて暗号化し、

前記送信手段は、暗号化された該第一の暗号化鍵と、該第一の暗号化鍵により暗号化された情報と、該セッション制御サーバに対する該情報の復号化要求指示を送信することを特徴とする通信装置。

【請求項２】　ネットワークを介して複数の通信装置と他のセッション制御サーバと通信可能に接続され、発信側の通信装置あるいは他のセッション制御サーバから送信された信号を受信し、受信した信号を着信側の通信装置あるいは他のセッション制御サーバに送信することで、該発信側の通信装置と該着信側の通信装置のセッションを確立させるセッション制御サーバにおいて、

暗号化された第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を復号化する手段と、

復号化した該第一の暗号化鍵を用いて、情報を復号化する手段とを備え、

前記受信手段が信号を受信すると、前記復号化手段は、復号化要求の有無、復号化対象の情報を判断し、第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化するか、あるいは、該第二の暗号化携に対応した第二の復号化鍵で該第一の暗号化鍵を復号化することで、復号化要求の有無を判断することを特徴とするセッション制御サーバ。

【請求項３】　請求項２記載のセッション制御サーバにおいて、

前記第一の暗号化鍵をセッション単位に保管もしくは記憶する手段を備え、

該第一の暗号化鍵を同一セッション内で、情報の復号化に再利用することを特徴とするセッション制御サーバ。

【請求項４】　ネットワークを介してセッション制御サーバと通信可能に接続され、前記セッション制御サーバとの間で信号送受信を行うことで、他の通信装置とのセッションを確立する通信装置において、

暗号化した第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を復号化する手段と、

得られた該第一の暗号化鍵により情報を復号化する手段と、

該第一の暗号化鍵をセッション単位に保管あるいは記憶する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、

同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用することを特徴とする着信側の通信装置。

【請求項５】　請求項１記載の通信装置において、

前記第一の暗号化鍵をセッション単位に保管あるいは記憶する手段と、

該第一の暗号化鍵を用いて情報を暗号化する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、

該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、

該第一の暗号化鍵を用いて情報を復号化する手段とを備え、

同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用することを特徴とする発信側の通信装置。

【請求項６】　請求項４または５記載の通信装置において、

セッション単位に管理した前記第一の暗号化鍵を、周期的に更新する手段を備え、

該周期的更新手段は、新規に該第一の暗号化鍵を生成する手段と、

該第一の暗号化鍵を、任意の第二の暗号化鍵により暗号化する暗号化鍵暗号化手段と、

任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と
からなることを特徴とする通信装置。

【請求項７】　請求項３記載のセッション制御サーバにおいて、

セッション単位に管理した前記第一の暗号化鍵を、周期的に更新する手段を備え、

該周期的更新手段は、任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段とからなることを特徴とするセッション制御サーバ。

【請求項８】　ネットワークを介して互いに通信可能に接続され、信号送受信を行うことで、セッションを確立する通信システムにおいて、

送信信号の守秘性を保持するために暗号化した情報を含む信号を送信する際に、暗号化のための第一の暗号化鍵を生成する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵を任意の第二の暗号化鍵で暗号化する暗号化鍵暗号化手段と、任意の第二の暗号化鍵で暗号化した第一の暗号化鍵を添付した、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、前記暗号化鍵暗号化手段は、該第一の暗号化鍵を、送信先の通信装置または１以上の該セッション制御サーバの各々が保有する第二の暗号化鍵を用いて暗号化し、前記送信手段は、暗号化された該第一の暗号化鍵と、該第一の暗号化鍵により暗号化された情報を含む信号と、該セッション制御サーバに対する復号化要求指示を送信する第１の通信装置と、

暗号化した第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、得られた該第一の暗号化鍵により情報を復号化する手段と、該第一の暗号化鍵をセッション単位に保管あるいは記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用する第２の通信装置と、

暗号化された第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、復号化した該第一の暗号化鍵を用いて、情報を復号化する復号化手段とを備え、前記受信手段が信号を受信すると、前記復号化手段は、復号化要求の有無を判断し、第二の暗号化鍵に対応した第二の復号化鍵で該第一の暗号化鍵を復号化するか、あるいは、該第二の暗号化携に対応した第二の復号化鍵で該第一の暗号化鍵を復号化することで、復号化要求の有無を判断するセッション制御サーバと

を有することを特徴とした通信システム。

【請求項９】　ネットワークを介して互いに通信可能に接続され、信号送受信を行うことで、セッションを確立する通信システムにおいて、

暗号化した第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を復号化する手段と、得られた該第一の暗号化鍵により情報を復号化する手段と、該第一の暗号化鍵をセッション単位に保管あるいは記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とを備え、同一セッション内の情報の暗号化および復号化に、前記第一の暗号化鍵を利用する着信側の通信装置と、

請求項１に記載の各手段に加え、前記第一の暗号化鍵をセッション単位に保管あるいは記憶する手段と、該第一の暗号化鍵を用いて情報を暗号化する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段と、該第一の暗号化鍵で暗号化された情報を含む信号を受信する手段と、該第一の暗号化鍵を用いて情報を復号化する手段とを備え、同一セッション内の情報の暗号化および復

号化に、前記第一の暗号化鍵を利用する発信側の通信装置と、

請求項２に記載の各手段に加え、前記第一の暗号化鍵をセッション単位に保管もしくは記憶する手段を備え、該第一の暗号化鍵を同一セッション内で、情報の復号化に再利用するセッション制御サーバと

を有することを特徴とした通信システム。

【請求項１０】　ネットワークを介して互いに通信可能に接続され、信号送受信を行うことで、セッションを確立する通信システムにおいて、

請求項４または５記載の各手段に加えて、セッション単位に管理した前記第一の暗号化鍵を、周期的に更新する手段を備え、該周期的更新手段は、新規に該第一の暗号化鍵を生成する手段と、該第一の暗号化鍵を、任意の第二の暗号化鍵により暗号化する暗号化鍵暗号化手段と、任意の第二の暗号化鍵で暗号化した該第一の暗号化鍵を添付し、かつ該第一の暗号化鍵で暗号化された情報を含む信号を送信する手段とからなる通信装置と、

請求項２記載の各手段に加えて、前記第一の暗号化鍵を周期的に更新する手段と、前記第一の暗号化鍵をセッション単位に保管もしくは記憶する手段を備え、該第一の暗号化鍵を同一セッション内で、情報の復号化に再利用するセッション制御サーバと

を有することを特徴とした通信システム。

【請求項１１】　通信装置で生成したセッション制御信号が、信頼されるセッション制御サーバと、信頼されないセッション制御サーバ経由で他の通信装置に送信される通信方法において、

信頼されるセッション制御サーバは、該通信装置から送信された信号を受信すると、復号化判断手段により復号化要求の有無を判断し、要求があれば、暗号化鍵復号化手段により第一の暗号化鍵の復号化を行い、復号化された該第一の暗号化鍵を用いて信号復号化手段により情報を復号化し、該情報を信頼されないセッション制御サーバに送信し、該セッション制御サーバは、これを受信し、前と同一処理を施して着信側通信装置に送信し、該着信側通信装置は、受信した信号の情報が第一の暗号化鍵で暗号化されており、かつ該第一の暗号化鍵が暗号化されて添付されているときは、自身の第二の暗号化鍵に対応する第二の復号化鍵を用

いて暗号化鍵復号化手段により復号化し、第一の暗号化鍵を取得し、該第一の暗号化鍵を用いて暗号化された情報を信号復号化手段により復号化することを特徴とする通信方法。

【請求項１２】　セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を元にＮＡＴ／ファイヤウォール装置のフィルタリング条件を変更する通信方法において、

セッション制御サーバは、通信装置の主情報通信径路のＩＰアドレスとポート番号を元に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、不特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケットを通過させ、その後、他の通信装置から受信した暗号化情報を第一暗号化鍵を用いて復号化し、該通信装置の主情報通信径路のＩＰアドレスとポート番号を元に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケットを通過させ、その後、通信装置からメッセージの切断信号を受信すると、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求し、指定ＩＰアドレスから指定ＩＰアドレスおよびポート番号宛のパケットを不通過とさせることを特徴とする通信方法。

【請求項１３】　セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を元に、暗号化された主情報について通信記録を可能にする通信方法において、

セッション制御サーバは、通信装置の主情報通信径路のＩＰアドレスとポート番号を元に、ＮＡＴ／ファイヤウォール装置に対して、フィルタリング条件変更要求に加えて、主情報転送を指示し、該ＮＡＴ／ファイヤウォール装置から主情報を受信すると、取得済みの主情報暗号化の鍵情報を用いて主情報復号化手段により復号化を行い、復号化が終了すると、復号化された状態の主情報とその鍵情報を記録することを特徴とする通信方法。

【請求項１４】　通信装置で生成したセッション制御信号が、信頼されるセッション制御サーバと、信頼されないセッション制御サーバ経由で他の通信装置に送信されるセッション制御用プログラムであって、

信頼されるセッション制御サーバのコンピュータに、該通信装置から送信された信号を受信する手順、復号化判断手段により復号化要求の有無を判断する手順、要求があれば、暗号化鍵復号化手段により第一の暗号化鍵の復号化を行う手順、復号化された該第一の暗号化鍵を用いて信号復号化手段により情報を復号化する手順、該情報を含む信号を信頼されないセッション制御サーバに送信する手順を、それぞれ実行させるためのセッション制御用プログラム。

【請求項１５】　セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を元にＮＡＴ／ファイヤウォール装置のフィルタリング条件を変更するセッション制御用プログラムであって、

セッション制御サーバのコンピュータに、通信装置の主情報通信径路のＩＰアドレスとポート番号を元に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順、不特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケットを通過させる手順、その後、他の通信装置から受信した暗号化情報を第一暗号化鍵を用いて復号化する手順、該通信装置の主情報通信径路のＩＰアドレスとポート番号を元に、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順、特定ＩＰアドレスから特定ＩＰアドレスおよびポート番号宛のパケットを通過させる手順、その後、通信装置からメッセージの切断信号を受信する手順、ＮＡＴ／ファイヤウォール装置に対してフィルタリング条件の変更を要求する手順、指定ＩＰアドレスから指定ＩＰアドレスおよびポート番号宛のパケットを不通過とさせる手順を、それぞれ実行させるためのセッション制御用プログラム。

【請求項１６】　セッション制御サーバがセッション確立中、あるいは、セッション変更中に得られた情報を元に、暗号化された確情報について通信記録を可能にするセッション制御用プログラムであって、

セッション制御サーバのコンピュータに、通信装置の主情報通信径路のＩＰアドレスとポート番号を元に、ＮＡＴ／ファイヤウォール装置に対して、フィルタリング条件変更要求に加えて、主情報転送を指示する手順、該ＮＡＴ／ファイヤウォール装置から主情報を受信する手順、取得済みの主情報暗号化の鍵情報を用いて主情報復号化手段により復号化を行う手順、復号化が終了すると、復号化さ

れた状態の主情報とその鍵情報を記録する手順を、それぞれ実行させるためのセッション制御用プログラム。

【請求項１７】　請求項１４から１６までのいずれかに記載のプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、信号の中継を行うセッション制御サーバ、暗号鍵に基づいて暗号化された通信を行う通信装置と通信システム、およびその通信方法、ならびにそのプログラムとそれを記録した記録媒体に関する。

【０００２】

【従来の技術】

従来より、ユーザ間の通信情報の暗号化方式としては、ＩＰＳｅｃ（Ｓｅｃｕｒｉｔｙ ａｒｃｈｉｔｅｃｔｕｒｅ ｆｏｒ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）、ＴＬＳ（Ｔｒａｎｓｐｏｒｔ Ｌａｙｅｒ Ｓｅｃｕｒｉｔｙ）、Ｓ／ＭＩＭＥが挙げられる。

中継サーバが、情報を参照できる暗号化方式としては、ＩＰＳｅｃ、ＴＬＳがある。

ＩＰＳｅｃは、ＴＣＰ／ＩＰの通信のセキュリティを強化するための技術であって、データをＩＰカプセル化してトンネリングする手法を規定するＥＳＰ（Ｅｎｃａｐｓｕｌａｔｉｏｎ Ｓｅｃｕｒｅ Ｐａｙｌｏａｄ）、ユーザ認証用のデータをＩＰデータに組み込むＡＨ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｈｅａｄｅｒ）などがある。ＴＬＳは、バンキングシステムなど、クライアント・サーバ間のセキュリティが必要なアプリケーションで広く用いられる。

【０００３】

ＩＰＳｅｃ，ＴＬＳの方法では、転送区間の始点、終点間で、暗号化鍵や方式の調整を行い、その結果に基づく暗号化通信を行い、通信装置が送受する伝達情報の機密性を向上させている。

上記に関しては、インターネットの標準化機関であるＩＥＴＦ（Ｉｎｔｅｒｎ

ｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）がとりまとめている規格書の中で、ＲＦＣ（Ｆｒｅｑｕｅｓｔ　ｆｏｒ　Ｃｏｍｍｅｎｔｓ）３２６１　Ｓｅｃｔｉｏｎ２６．２（非特許文献１参照）がある。

【０００４】

【非特許文献１】

ＲＦＣ３２６１Ｓｅｃｔｉｏｎ２６．２

【０００５】

【発明が解決しようとする課題】

ＩＰＳｅｃやＴＬＳなどの暗号化方式では、転送区間の始点、終点間で暗号化方式、鍵の調整を行い、暗号化／復号化の処理を転送区間の始点、終点で行う必要があった。そのため、信号中継を行うセッション制御サーバで、必ず情報の復号化を行うことになり、セッション制御サーバに対する情報保護が可能な暗号化通信が困難であった。

また、Ｓ／ＭＩＭＥの暗号化方式では、発着通信装置間で暗号化を行い、全てのセッション制御サーバに対して情報保護が可能であるが、特定のセッション制御サーバに情報開示が必要な場合であっても、情報開示が不可能であるという問題点があった。

【０００６】

（目的）

本発明の目的は、上記のような従来の課題を解決し、発着ユーザ間通信のエンド・エンド間の機密性を確保しながら、かつ、情報開示が必要な特定のセッション制御サーバに対してのみ情報開示を可能とするセッション制御サーバ、通信装置、通信システムおよび通信方法、ならびにそのプログラムと記録媒体を提供することにある。

【０００７】

【課題を解決するための手段】

本発明は、

（１）通信装置Ａがセッション確立のための信号送信に先立ち、信号内の情報の暗号化のための第一の暗号化鍵（対称暗号鍵）を生成する。

送信先の通信装置Ｂの第二の暗号化鍵（公開鍵あるいは事前共有鍵）と、通信装置Ａがセッション確立に伴い情報を開示する対象である０以上のセッション制御サーバの第二の暗号化鍵（公開鍵あるいは事前共有鍵）を用いて、個々の第二の暗号化鍵毎に第一の暗号化鍵を暗号化する。

通信装置Ａは、第一の暗号化鍵で暗号化した情報とともに、各第二の暗号化鍵（個々の公開鍵あるいは事前共有鍵）で暗号化した第一の暗号化鍵と、復号化要求指示をセッション制御サーバに送信する。

【０００８】

なお、ここでの復号化要求指示は、通信装置Ａがセッション確立に伴い情報を開示する対象であるセッション制御サーバを、セッション制御サーバを示す識別子の形で陽に提示していてもよいし、陽に提示していなくてもよい。

また、復号化対象のコンテンツＩＤについても、陽に提示していてもよいし、陽に提示していなくてもよい。

陽に提示していない場合においては、例えばセッション確立に伴い経由される個々のセッション制御サーバにおいて、自らの保持する第二の暗号化鍵に対応する第二の復号化鍵による第一の暗号化鍵の復号化を行い、得られた情報が第一の暗号化鍵を示す表現形式に合致しているとき、自らを復号化要求を受けたセッション制御サーバと判断できるため、第二の暗号化鍵で暗号化された第一の暗号化鍵自身が復号化要求指示となる（請求項１参照）。

【０００９】

（２）通信装置Ａもしくは他のセッション管理サーバが送信した信号を受信したセッション制御サーバは、復号化要求有無、復号化対象の情報を判断し、復号化要求があった場合に、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵の復号化を行う。もしくは、自らの第二の暗号化鍵に対応する第二の復号化鍵により第一の暗号化鍵の復号化を行い、その結果から復号化要求有無を判断する。または、これらのいずれをも行う。これらは、（１）記載の通信装置における復号化要求に依存する。

いずれの場合においても、得られた第一の暗号化鍵を用いて、暗号化情報の復号化を行う（請求項２参照）。

【００１０】

（３）上記（２）のセッション制御サーバは、更に暗号化した第一の暗号化鍵を、セッション単位に保管もしくは記憶する。その後、当該セッションの情報の復号化の際に再利用する（請求項３参照）。

（４）通信装置Ｂは、暗号化した第一の暗号化鍵を添付した暗号化情報を含む信号を受信し、第一の暗号鍵の復号化を行い、その鍵を用いて、暗号化情報の復号化を行う。通信装置Ｂは、セッション単位に第一の暗号化鍵を保管もしくは記憶し、同一セッション内の情報の暗号化に、前記第一の暗号化鍵を再利用する。

第一の暗号化鍵を暗号化した情報が添付されない暗号化情報を含む信号を送信する。第一の暗号化鍵は、同一セッション内の情報の復号化にも再利用する（請求項４参照）。

【００１１】

（５）通信装置Ａは、セッション単位に第一の暗号化鍵を保管もしくは記憶し、第一の暗号化鍵を暗号化した情報が添付されない暗号化情報を含む信号を受信した際に、同一セッション内の情報の復号化に、および、同一セッション内の情報の暗号化に、前記第一の暗号化鍵を再利用する（請求項５参照）。

（６）通信装置Ａおよび通信装置Ｂは、セッション内で、一定時間あるいは一定回数使用経過後、第一の暗号化鍵を更新し、更新信号とともに送信する（請求項６参照）。

（７）セッション制御サーバは、セッション内で通信装置Ａ（あるいは通信装置Ｂ）より、第一の暗号化鍵の更新信号を受信すると、保管あるいは記憶していたそのセッションの第一の暗号化鍵を更新し、更新信号とともに通信装置Ｂ（あるいは通信装置Ａ）に送信する（請求項７参照）。

【００１２】

本発明においては、情報開示を行うセッション制御サーバを指定して、情報開示を行いながら安全な信号の送受信が可能となる。通信装置間の暗号化情報を含む信号通信の場合でも、特定のセッション制御サーバが信号情報の参照が可能となるため、その情報を基に通信制御が可能となることである。

【００１３】

【発明の実施の形態】

以下、本発明の実施形態を、図面により詳細に説明する。

（システム構成）

図１は、本発明の実施形態に係る通信システムの構成図である。

図１に示すように、本通信システム１００は、複数のセッション制御サーバ１０１と、複進の通信装置１０２とＮＡＴ／ファイヤウォール装置１０３、およびネットワーク１０を含むように構成される。

なお、通信装置１０２は、本発明による手順に従いセッション制御サーバ１０１を介して暗号化情報を含む信号により通信を行う。なお、通信システム１００においては、セッション制御サーバ１０１は２台に限定されるものではない。ここでは、通信装置１０２が２台示されているが、２台に限定されるものではない。ＮＡＴ／ファイヤウォール装置１０３が１台示されているが、１台に限定されるものではない。

【００１４】

なお、本発明によれば、通信装置１０２はパソコン、携帯端末、あるいはゲートウェイなどの通信機器を含み、ネットワーク１０の構成は、有線、無線を問わない。以降は、説明の便宜を図るため、通信装置１０２－１を発信側とし、通信装置１０２－２を着信側として説明する。また、セッション制御サーバ１０１－１を発信側、セッション制御サーバ１０１－２を着信側として説明する。

通信装置１０２－１が暗号化情報とともに通信装置１０２－２用に暗号化した第一の暗号化鍵とセッション制御サーバ１０１－１用に暗号化した第一の暗号化鍵を、セッション制御サーバ１０１－１に送信する。

【００１５】

セッション制御サーバ１０１－１が通信装置１０２－１から送信された暗号化情報と２つの暗号化した第一の暗号化鍵を受信し、これらのうちセッション制御サーバ用情報を復号化し、得られた第一の暗号化鍵で暗号化情報を復号化し、情報の参照が可能となる。

この際に、セッション制御サーバ１０１－１は、参照した情報をもとにＮＡＴ／ファイヤウォール装置１０３に対して、フィルタリング条件の変更要求を送信

してもよい。ＮＡＴ／ファイヤウォール装置１０３からフィルタリング条件の変更完了通知を受信した後、セッション制御サーバ１０１－１は通信装置１０２－１から受信した暗号化情報を含む信号と２つの第一の暗号化鍵を、セッション制御サーバ１０１－２に送信する。

【００１６】

セッション制御サーバ１０１－２は、セッション制御サーバ１０１－１から送信された暗号化情報と２つの暗号化した第一の暗号化鍵を受信するが、これらを復号化できないため、暗号化された情報の参照はできない。セッション制御サーバ１０１－２は、受信した暗号化情報と２つの暗号化した第一の暗号化鍵を通信装置１０２－２に送信する。

通信装置１０２－２は、セッション制御サーバ１０１－２から受信した通信装置１０２－２用情報を復号化し、得られた第一の暗号化鍵で暗号化した情報を復号化することで、情報の参照が可能となる。

通信装置１０２－２は、通信装置１０２－１に送信すべき応答信号などの信号をセッション対応に記憶している第一の暗号化鍵を再利用して、暗号化し、セッション制御サーバ１０１－１，１０１－２経由で、あるいは直接、通信装置１０２－１に送信する。

【００１７】

（通信装置）

図３は、本発明の実施形態に係る通信装置のブロック構成図である。

図３に示すように、通信装置１０２は、信号送信手段１２０、セッション制御手段１２１、暗号化鍵生成手段１２２、暗号化鍵暗号化手段１２３、信号情報暗号化手段１２４、暗号化鍵再利用手段１２５、信号情報復号化手段１２６、暗号化鍵復号化手段１２７、信号受信手段１２８、暗号化鍵更新手段１２９を含むように構成される。

通信装置１０２－１は、セッション制御手段１２１で生成された信号のうち、機密性が必要な情報を、暗号化鍵生成手段１２２で生成された第一の暗号化鍵を使用して、信号暗号化手段１２４で暗号化する。

【００１８】

そして、その第一の暗号化鍵を、開示先通信装置およびサーバの第二の暗号化鍵（例えば、実施形態においては公開鍵とする）を使用して、暗号化鍵暗号化手段１２３により各々暗号化する。その際に、使用した第一の暗号化鍵は、暗号化鍵再利用手段１２５にてセッション識別子対応に保管もしくは記憶される。

セッション制御手段１２１で生成された情報のうち、暗号化していない情報に、セッション制御サーバ１０１および送信先通信装置に復号化を要求する情報を追加し、第一の暗号化鍵で暗号化した情報と、復号化要求対象が保持する第二の暗号化鍵により暗号化した第一の暗号化鍵とともに、信号送信手段１２０にて、セッション制御サーバ１０１－１に送信する。これにより、機密性が必要な情報について、特定のセッション制御サーバ１０１－１と通信装置１０２－２に対してのみ開示可能な状態で、信号送信が可能になる。

【００１９】

図４は、本発明の実施形態に係る通信装置１０２－１の送信信号例を示す図である。

通信装置１０２－１は、機密性が必要な情報を第一の暗号化鍵を使用して暗号化する。その第一の暗号化鍵を、開示先通信装置およびサーバの各々の第二の暗号化鍵を使用して各々暗号化する。暗号化していない情報に、セッション制御サーバ１０１に復号化要求する情報を追加する。第一の暗号化鍵で暗号化した情報と、復号化要求対象が保持する第二の暗号化鍵により暗号化した第一の暗号化鍵とともに、信号送信手段１２０にて、セッション制御サーバ１０１－１に送信する。

この送信信号例については、さらに、第１の実施形態の説明で図６とともに説明する。

【００２０】

図５は、本発明の実施形態に係る通信装置１０２－２の送信信号例を示す図である。

この送信信号例については、さらに、第１の実施形態の説明で、図６とともに説明する。

【００２１】

（セッション制御サーバ）

図２は、本発明の実施形態に係るセッション制御サーバのブロック構成図である。

図２に示すように、セッション制御サーバ１０１は、信号受信手段１１０、復号化判断手段１１１、暗号化鍵復号化手段１１２、復号化鍵再利用手段１１３、信号情報復号化手段１１４、セッション制御手段１１５、信号送信手段１１６を具備している。ＮＡＴ／ファイヤウォール制御手段１１７、主情報通信受信手段１１８、主情報復号化手段１１９を具備している。

【００２２】

暗号化鍵復号化手段１１２は、第一の暗号化鍵の格納されたデータを見て、どの第二の暗号化鍵に対応した第二の復号化鍵を使用して、復号化するかを判断した上で、第一の暗号化鍵の復号化を行い、情報復号化手段１１４に復号化鍵を渡す。情報信号の復号化により、通信装置間の制御情報が参照可能となり、セッション制御手段１１５に必要な情報を提供する。

復号化鍵は、セッション制御手段１１５内の識別子に対応して、復号化鍵再利用手段１１３において、信号情報に含まれるセッションの識別子に対応して、復号化鍵を保管もしくは記憶する。

セッション制御手段１１５で信号送信の準備が整うと、信号受信手段１１０で受信した暗号化した情報と、暗号化した第一の暗号化鍵を含む信号を、信号送信手段１１６により通信装置１０２－２に送信する。

【００２３】

（第１の実施形態）

図６は、本発明の第１の実施形態に係る通信方法の説明図である。

第１の実施形態では、通信装置１０２－１で生成したセッション制御信号が、通信装置１０２－１から信頼されるセッション制御サーバ１０１－１、信頼されないセッション制御サーバ１０１－２経由で通信装置１０２－２に送信される例を説明する。

例えば、図４に示すように、通信装置１０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッド４００で

あって、そのメッセージに含まれる通信装置間の制御情報（ＳＤＰ：Ｓｅｓｓｉｏｎ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）４０５が暗号化されている。ＳＤＰには、通信装置１０２－１の主情報通信の情報として、受信用ＩＰアドレス、ポート番号などを含む。改ざん防止のために、暗号化情報４０４に、通信装置１０２－１のユーザのデジタル署名を添付してもよい。

【００２４】

ＳＩＰメッセージは、セッション制御サーバ１０１－１、および、セッション制御サーバ１０１－２を経由して、通信装置１０２－２に送信されるものである。暗号化した情報は、Ｓ／ＭＩＭＥのＥｎｖｅｌｏｐｅｄ－Ｄａｔａ４０４として設定する。その暗号化に使用した鍵（第一の暗号化鍵）は、セッション制御サーバ１０１の公開鍵と、着ユーザの公開鍵（第二の暗号化鍵）とで各々暗号化し、Ｅｎｖｅｌｏｐｅｄ－Ｄａｔａの中のＲｅｃｅｐｉｅｎｔＩｎｆｏ４０６として設定する。

また、第一の暗号化鍵は、セッション制御サーバ１０１－１と通信装置１０２－１間の事前共有鍵や、通信装置１０２－１と通信装置１０２－２のユーザ間の事前共有鍵で、各々暗号化されてもよい。

【００２５】

そして、ＳＩＰメッセージ内の暗号化していない範囲４０１に、セッション制御サーバに復号化要求を示す値と、復号化すべきコンテンツＩＤとを含む。

改竄防止が必要なＳＩＰメッセージ４０２に対して、通信装置１０２－１のユーザのデジタル署名４０３を添付してもよい。

セッション制御サーバ１０１－１は、通信装置１０２－１から送信されたＩＮＶＩＴＥメソッド４００を信号受信手段１１０にて受信する。復号化判断手段１１１において、復号化要求パラメータ（例：Ｓｅｓｉｏｎ－Ｐｏｌｉｃｙ）の値で、復号化要求を判断するか、暗号化された第一暗号化鍵が設定されたＲｅｃｅｐｉｅｎｔＩｎｆｏ４０６の復号化可否で、復号化要求を判断してもよい。

【００２６】

復号化要求がある場合、暗号化鍵復号化手段１１２は、指定されたコンテンツＩＤの示すデータ４０４の中の、第一の暗号化鍵の格納されたデータ（Ｒｅｃｅ

ｐｉｅｎｔＩｎｆｏ）４０６の型を見て、どの第二の暗号化鍵に対応した第二の復号化鍵を使用して復号化するかを判断した上で、第一の暗号化鍵の復号化を行い、信号復号化手段１１４に復号化鍵を渡す。暗号化情報４０５の復号化により、通信装置間制御用の信号が参照可能となり、セッション制御手段１１５に必要な情報を提供する。

復号化要求がない場合や、指定されたコンテンツＩＤが設定されてない場合は、復号化処理は行わない。

【００２７】

セッション制御サーバ１０１－１は、復号化要求の有無にかかわらず、セッション制御手段１１５において、通信装置１０２－１から受信したＩＮＶＩＴＥメソッドについて、処理（必要なパラメータ変更など）を行い、信号送信手段１１６よりセッション制御サーバ１０１－２に送信する。

セッション制御サーバ１０１－２は、セッション制御サーバ１０１－１から送信されたＩＮＶＩＴＥメソッドを信号受信手段１１０にて受信する。

復号化判断手段１１１において、復号化要求パラメータ（例：Ｓｅｓｉｏｎ－Ｐｏｌｉｃｙ）の値で復号化要求を判断するか、あるいは暗号化された第一暗号化鍵が設定されたＲｅｃｅｐｉｅｎｔＩｎｆｏ４０６の復号化可否で、復号化要求を判断してもよい。

復号化要求がない、あるいは、復号化不可のため、暗号化された通信装置間の制御情報は参照できない。セッション制御手段１１５にて参照可能な情報をもとに、ＩＮＶＩＴＥメソッドについて処理（必要なパラメータ変更など）を行い、信号送信手段１１６より通信装置１０２－１に送信する。

【００２８】

信号を受信した通信装置１０２－２は、信号受信手段１２８で受信した信号の情報が第一の暗号化鍵で暗号化されており、第一の暗号化鍵が暗号化されて添付されていると、自身の第二の暗号化鍵に対応する第二の復号化鍵（第一の暗号化鍵が公開鍵の場合は秘密鍵、あるいは第二の暗号化鍵が事前共有鍵であれば同事前共有鍵）を使用して、暗号化鍵復号化手段１２７で復号化し、第一の暗号化鍵を得る。その第一の暗号化鍵を使用して、暗号化された情報を信号復号化手段１

２６にて復号化し、情報が参照可能となる。その情報をセッション制御手段１２１に提示する。

【００２９】

セッション制御手段１２１は、必要に応じて送信すべき情報を生成するとともに、暗号鍵を暗号化鍵再利用手段１２５にてセッション識別子対応に保管する。

例えば、図５に示すようなＩＮＶＩＴＥメソッドに対する応答信号として２００　ＯＫ　５００を送信する。送信すべき情報について、保管もしくは記憶している第一の暗号化鍵を使用して、信号暗号化手段１２４にて暗号化した情報５０５をＥｎｃｒｙｐｅｄ－Ｄａｔａとして設定し、信号送信手段１２０より信号を送信する。

また、改ざん防止のために、暗号化した情報５０４に対してデジタル署名を添付してもよい。

【００３０】

（応用例１：請求項６参照）

その後のセッションの継続信号が、例えばＭＥＳＳＡＧＥメソッドが通信装置１０２－１よりセッション制御サーバ１０１－１，１０１－２経由で通信装置１０２－２に送信される。通信装置１０２－１は、セッション単位に保管または記録している第一暗号化鍵を使用して、ＭＥＳＳＡＧＥメソッドに設定するインスタントメッセージの内容を暗号化する。第一暗号化鍵を添付しないで、暗号化した情報を含むＭＥＳＳＡＧＥメソッドを送信する。

当該信号を受信した通信装置１０２－２は、暗号化鍵再利用手段１２３において、セッション識別子をキーに保管している第一暗号化鍵を取得し、その第一暗号化鍵にて暗号化情報を復号化する。

【００３１】

（応用例２：請求項３参照）

セッション制御サーバ１０１－１においても、セッション単位に保管している第一の暗号化鍵を使用して暗号化情報を復号化する。

【００３２】

（応用例３：請求項６参照）

また、一定時間経過後、通信装置１０２－１がＭＥＳＳＡＧＥメソッドをセッション制御サーバ１０１－１，１０１－２経由で通信装置１０２－２に送信する際に、暗号化鍵更新手段１２９にて第一暗号化鍵を更新する。更新した暗号化鍵を用いて情報を暗号化し、Ｓ／ＭＩＭＥのＥｎｖｅｌｏｐｅｄ－Ｄａｔａとして設定する。

その暗号化に使用した鍵（更新した第一の暗号化鍵）は、セッション制御サーバの公開鍵と、着ユーザの公開鍵（第二の暗号化鍵群）とで各々暗号化し、Ｅｎｖｅｌｏｐｅｄ－Ｄａｔａの中のＲｅｃｅｐｉｅｎｔＩｎｆｏとして設定する。

更新した第一の暗号化鍵を添付した暗号化情報を含む信号を受信した通信装置１０２－２は、更新された第一の暗号化鍵を暗号化鍵再利用手段１２５にて保管あるいは記憶する。

【００３３】

（応用例４：請求項７参照）

更新した第一の暗号化鍵を添付した暗号化情報を含む信号を受信したセッション制御サーバ１０１－１は、更新された第一の暗号化鍵を暗号化鍵再利用手段１１３にて保管あるいは記憶する。

【００３４】

（第２の実施形態）

図７は、本発明の第２の実施形態に係る通信方法の説明図である。

ここでは、セッション制御サーバが、セッション確立中に得られた情報を元にＮＡＴ／ファイヤウォール装置１０３のフィルタリング条件を変更する例を示している。

例えば、セッション制御サーバが、通信装置１０２－１から受信した信号がＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであって、そのメッセージに含まれる通信装置間の制御情報（ＳＤＰ：Ｓｅｓｓｉｏｎ　Ｄｅｓｃｒｉｐｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）が暗号化されている。

第二の暗号化鍵に対応する第二の復号化鍵を使用して復号化することにより、制御情報に設定されている通信装置１０２－１の主情報通信径路のＩＰアドレスとポート番号などが参照可能となる。この情報を元に、ＮＡＴ／ファイヤウォー

ル制御手段１１７において、遠隔のＮＡＴ／ファイヤウォール装置１０３に対してフィルタリング条件の変更（不特定ＩＰアドレスから特定ＩＰアドレス＋ポート番号宛のパケット通過指示）を要求する。

【００３５】

その後、通信装置１０２－２から受信した信号が、ＳＩＰメッセージの１つである２００　ＯＫ　応答であって、そのメッセージに含まれる通信装置間の制御情報（ＳＤＰ）が暗号化されている。復号化鍵再利用手段１１３に記憶していた第一の暗号化鍵を用いて暗号化情報を復号化して、通信装置１０２－２の主情報通信径路のＩＰアドレスとポート番号が通信装置間の制御情報が参照可能となる。この情報を元に、ＮＡＴ／ファイヤウォール制御手段１１７において、遠隔のＮＡＴ／ファイヤウォール装置１０３に対してフィルタリング条件の変更（特定ＩＰアドレスから特定ＩＰアドレス＋ポート番号宛のパケット通過指示）を要求する。これにより、ＮＡＴ／ファイヤウォール装置１０３において、通信装置１０２－１と通信装置１０２－２間の主情報についてパケット通過が可能となる。

【００３６】

その後、通信装置１０２－１あるいは１０２－２から送信したＳＩＰメッセージの切断信号であるＢＹＥメソッドを受信すると、セッション制御サーバ１０１－１は、ＮＡＴ／ファイヤウォール制御手段１１７において、ＮＡＴ／ファイヤウォール装置１０３に対してフィルタリング条件の変更（指定ＩＰアドレスから指定ＩＰアドレス＋ポート番号宛のパケット不通過指示）を要求する。

本実施形態で示したように、通信装置より信号内の情報を安全に開示されたセッション制御サーバ１０１－１により、セッション単位にＮＡＴ／ファイヤウォール制御を行うことができるので、アクセス制御の精度を高めることが可能となる。情報を開示されないセッション制御サーバ１０１－２は、主情報の経路情報が参照できないため、主情報のモニタが困難となり、その結果、主情報通信の機密性を高めることができる。

【００３７】

（第３の実施形態）

図８は、本発明の第３の実施形態に係る通信方法の説明図である。

ここでは、セッション制御サーバ１０１－１が、セッション確立中に得られた情報を元に、暗号化された主情報についても、通信記録が可能となる例を説明する。

例えば、通信装置１０２－１からの送信信号は、ＲＦＣ３２６１に準拠したＳＩＰメッセージの１つであるＩＮＶＩＴＥメソッドであって、そのメッセージに含まれる通信装置情報ＳＤＰが暗号化されている。ＳＤＰには、通信装置１０２－１、通信装置１０２－２間に主情報通信の際に使用するＩＰアドレス、ポート番号に加えて、主情報暗号化のための鍵情報を含む。

セッション制御サーバ１０１－１が、主情報通信記録の手段（受信手段１１８）と、主情報復号化手段１１９を備え、遠隔のＮＡＴ／ファイヤウォール装置１０３に対して指示を送信する。

【００３８】

この指示は、前述の第２の実施形態で説明したフィルタリング条件変更要求に加えて、主情報転送を指示する。セッション制御サーバ１０１－１の主情報通信受信手段１１８にて、ＮＡＴ／ファイヤウォール装置１０３から主情報を受信する。主情報が暗号化されている場合、既に取得済みの主情報暗号化の鍵情報を用いて、主情報復号化手段１１９にて復号化を行う。

復号化が正常終了すると、復号化された主情報、あるいは、暗号化した状態の主情報とその鍵情報を記録する。

セッション制御サーバ１０１－２は、暗号化情報を復号化できないため、通信装置情報ＳＤＰは参照できず、ＳＤＰに含まれる主情報暗号化のための鍵情報は参照できない。そのため、ネットワーク内のモニタ装置で主情報をモニタしても、暗号化されており、それを復号化することができない。

このように、主情報が暗号化されている場合でも、セッション制御サーバによる復号化した主情報の記録が行えるため、通信情報の監査、および、記録が可能となる。

【００３９】

なお、第１の実施形態、第２の実施形態および第３の実施形態で説明した処理順序をプログラム化して、ＣＤ－ＲＯＭなどの記録媒体に格納しておけば、プロ

グラムの販売や貸与の際に便利であり、また、セッション制御サーバ１０１－１，１０１－２のコンピュータに記録媒体を装着して、プログラムをインストールし、これを実行させることで、本発明を容易に実現することができる。

【００４０】

このように、本実施形態に係る通信システムは、通信装置間だけでなく、信号中継を行うセッション制御サーバに対しても、情報開示が可能であるため、通信装置が送受信する伝達信号の機密性を高めながら、特定のセッション制御サーバによる通信制御が可能となる。

【００４１】

【発明の効果】

以上説明したように、本発明によれば、通信装置間の機密性の高い信号送受信を保証した上で、通信装置の要求に応じて特定のセッション制御サーバのみ、信号情報を開示することが可能である。また、通信装置間の接続構成によらず、信号情報を開示するセッション制御サーバの指定が可能となる。

【図面の簡単な説明】

【図１】

本発明の実施形態に係る通信システムのブロック構成図である。

【図２】

図１におけるセッション制御サーバの詳細な構成図である。

【図３】

図１における通信装置の詳細な構成図である。

【図４】

本発明の実施形態に係る通信装置１０２－１の送信信号例を示す図である。

【図５】

本発明の実施形態に係る通信装置１０２－２の送信信号例を示す図である。

【図６】

本発明の第１の実施形態に係る通信方法の説明図である。

【図７】

本発明の第２の実施形態に係る通信方法の説明図である。

【図８】

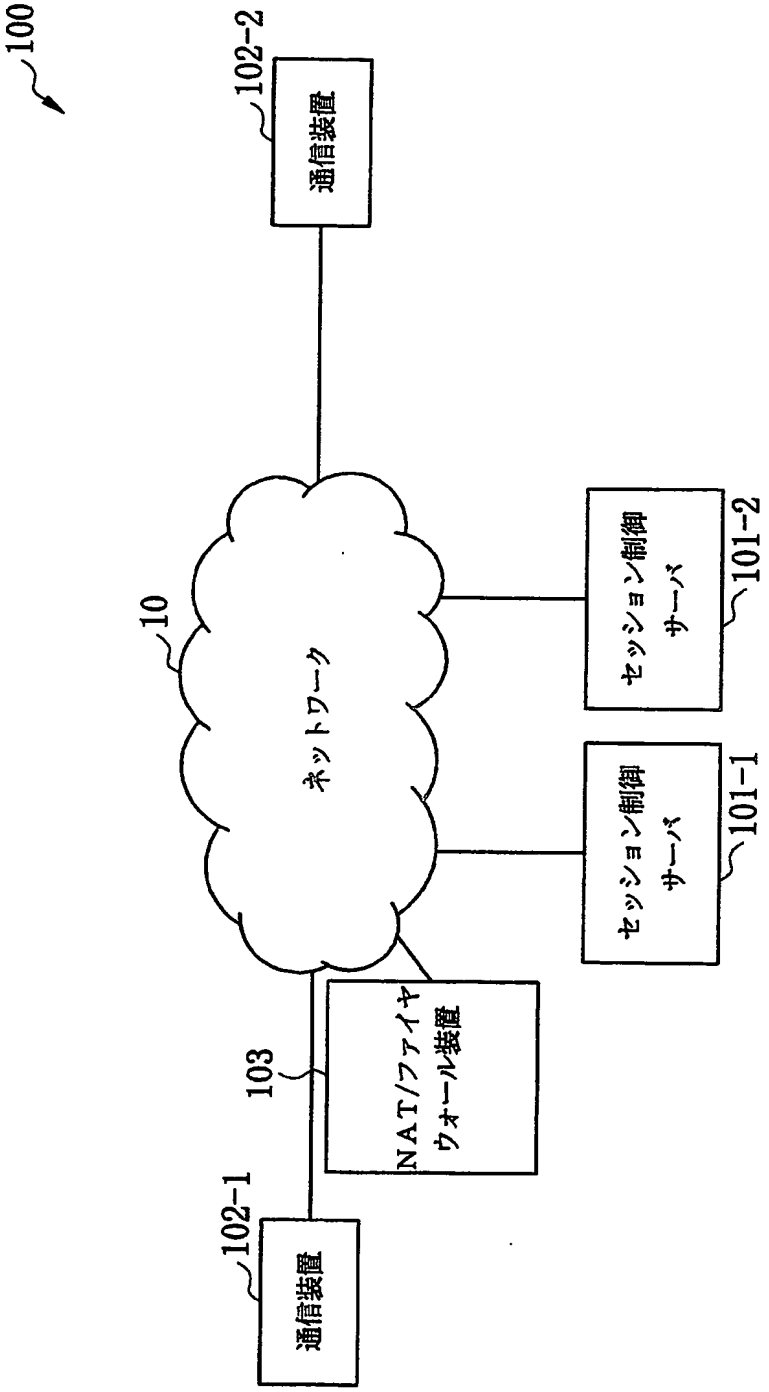
本発明の第３の実施形態に係る通信方法の説明図である。

【符号の説明】

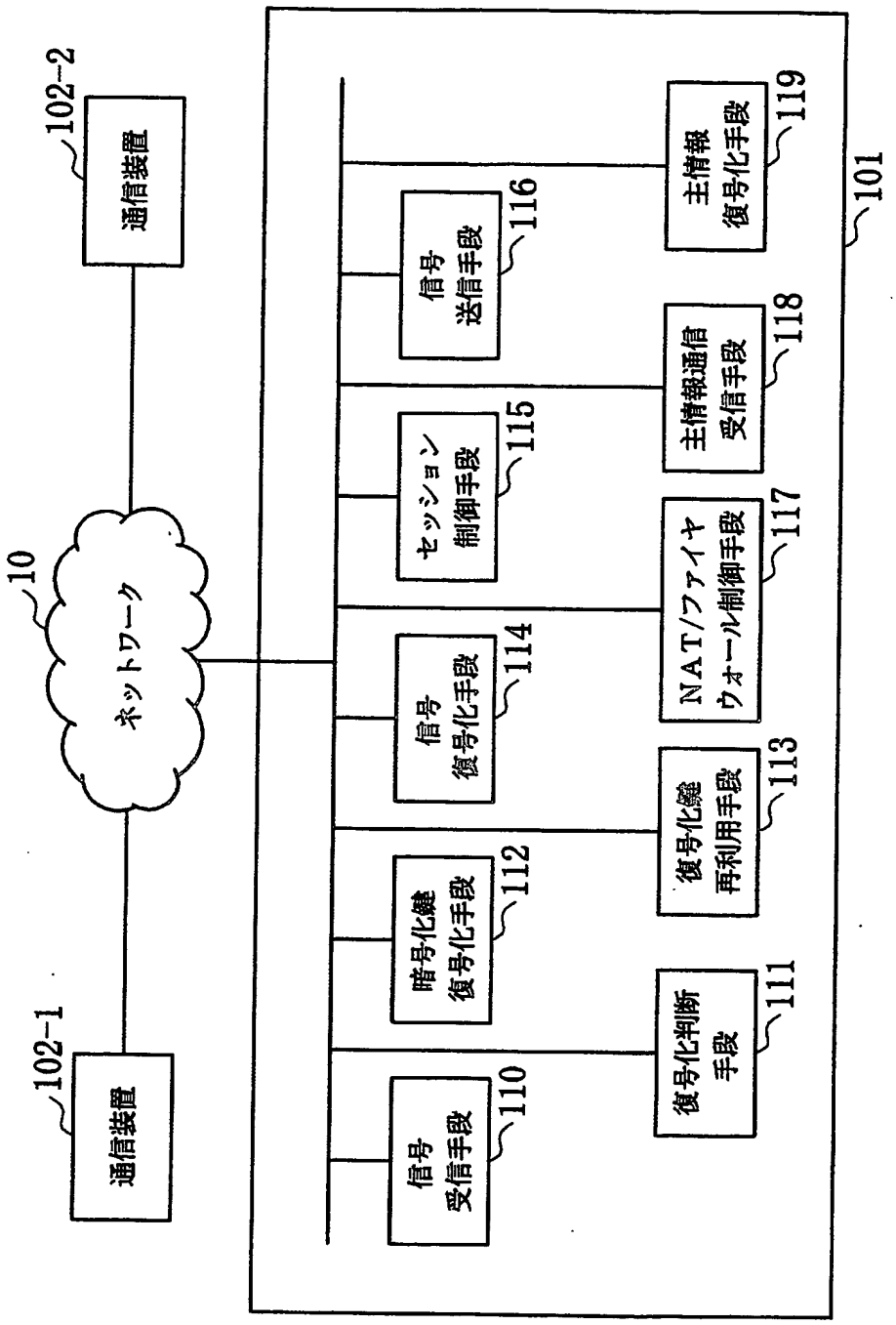
１０…ネットワーク、１０１－１，１０１－２…セッション制御サーバ、
１０２－１，１０２－２…通信装置、１１０…信号受信手段、
１１１…復号化判断手段、１１２…暗号化鍵復号化手段、
１１３…復号化鍵再利用手段、１１４…信号復号化手段、
１１５…セッション制御手段、１１６…信号送信手段、
１１７…ＮＡＴ／ファイヤウォール制御手段、１１８…主情報通信受信手段、
１１９…主情報復号化手段、１２０…信号送信手段、
１２１…セッション制御手段、１２２…暗号化鍵生成手段、
１２３…暗号化鍵暗号化手段、１２４…信号暗号化手段、
１２５…暗号化鍵再利用手段、１２６…信号復号化手段、
１２７…暗号化鍵復号化手段、１２８…信号受信手段、
１２９…暗号化鍵更新手段、
４００～４０６…通信装置１０２－１の送信信号領域、
５００～５０５…通信装置１０２－２の送信信号領域。

【書類名】　図面

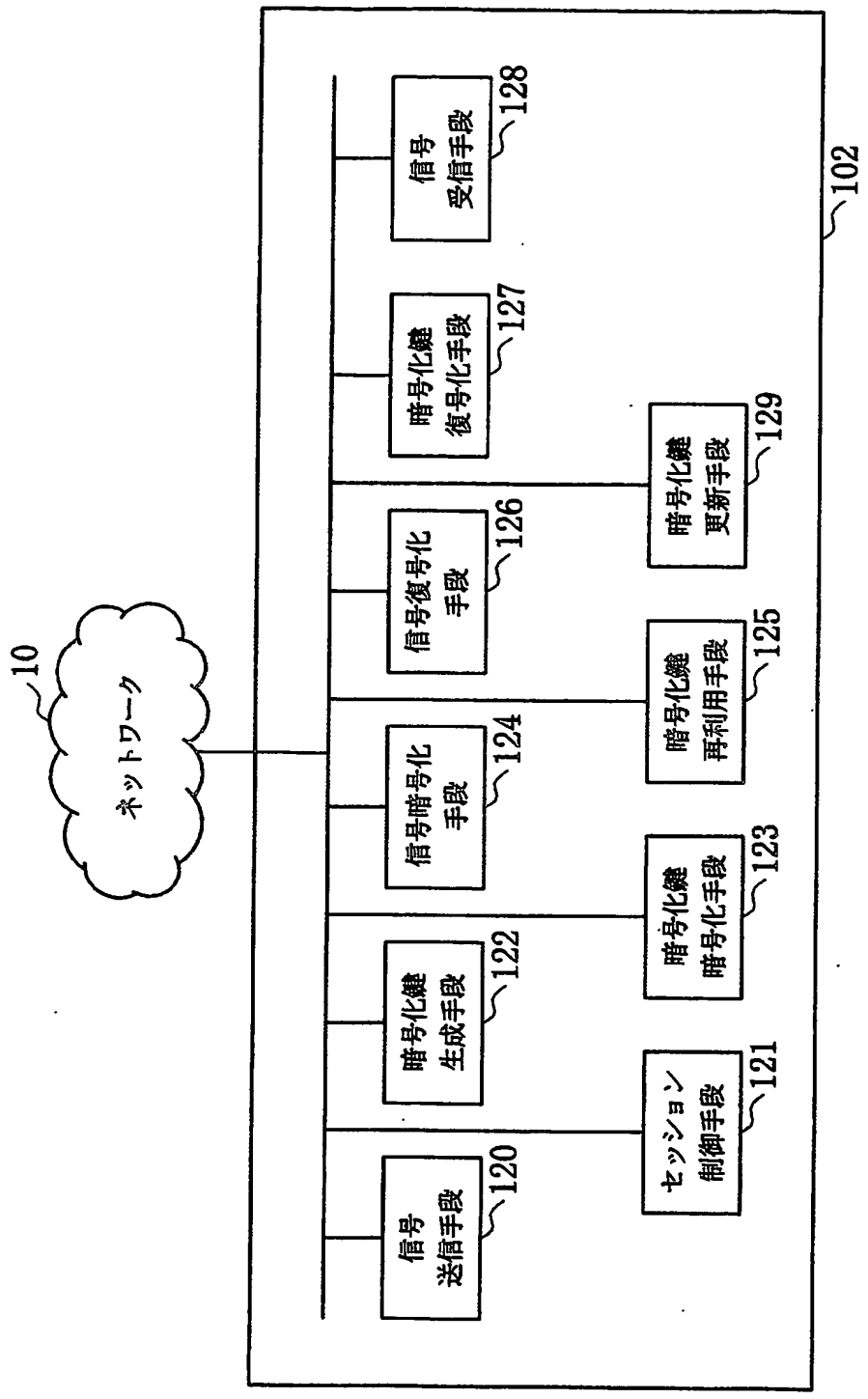
【図１】


100
102-2
通信装置
10
ネットワーク
セッション制御サーバ
101-2
セッション制御サーバ
101-1
NAT/ファイヤウォール装置
103
102-1
通信装置

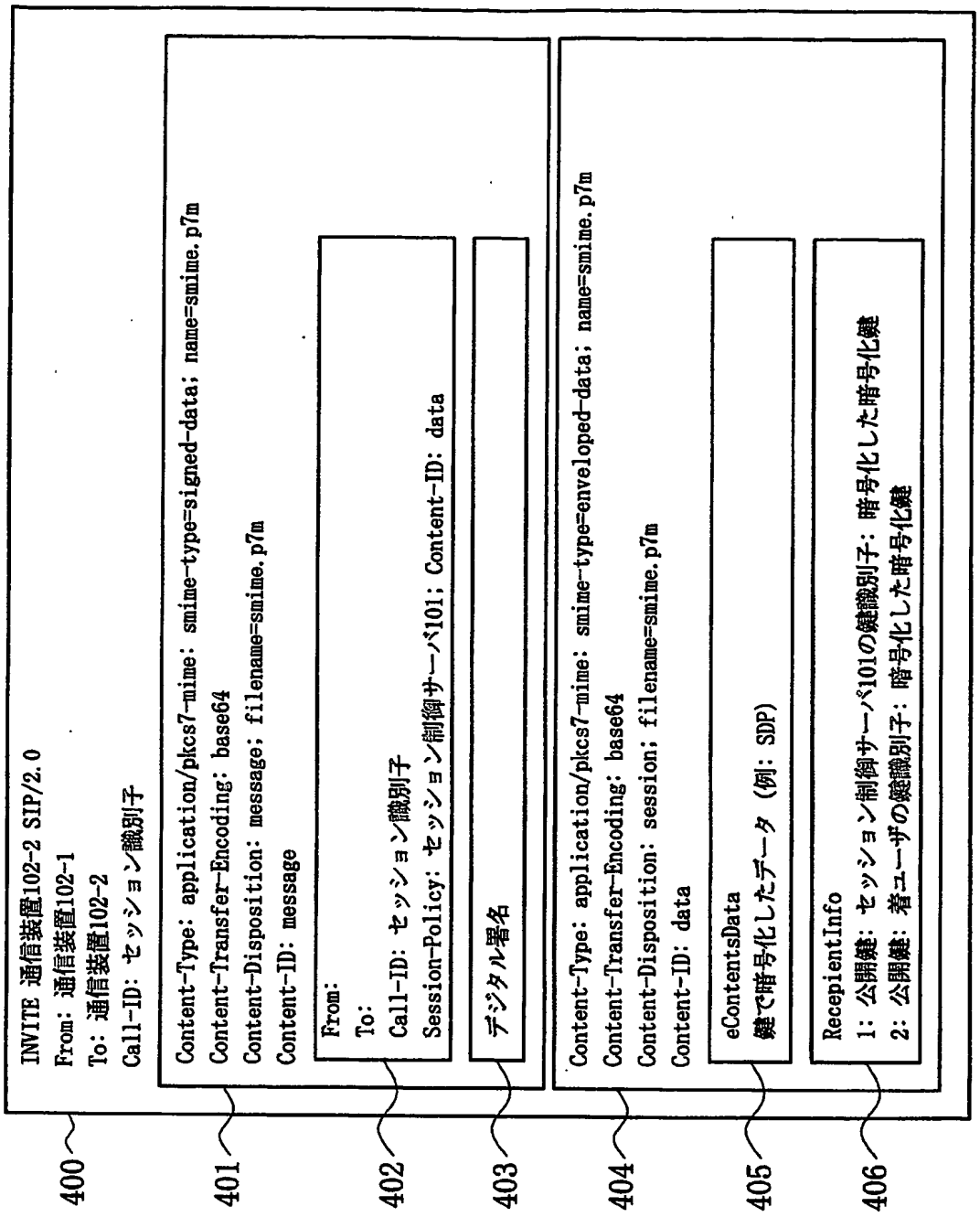
【図２】


102-2
通信装置
102-1
通信装置
10
ネットワーク
101
信号
受信手段
110
暗号化鍵
復号化手段
112
信号
復号化手段
114
セッション
制御手段
115
信号
送信手段
116
復号化判断
手段
111
復号化鍵
再利用手段
113
NAT/ファイヤ
ウォール制御手段
117
主情報通信
受信手段
118
主情報
復号化手段
119

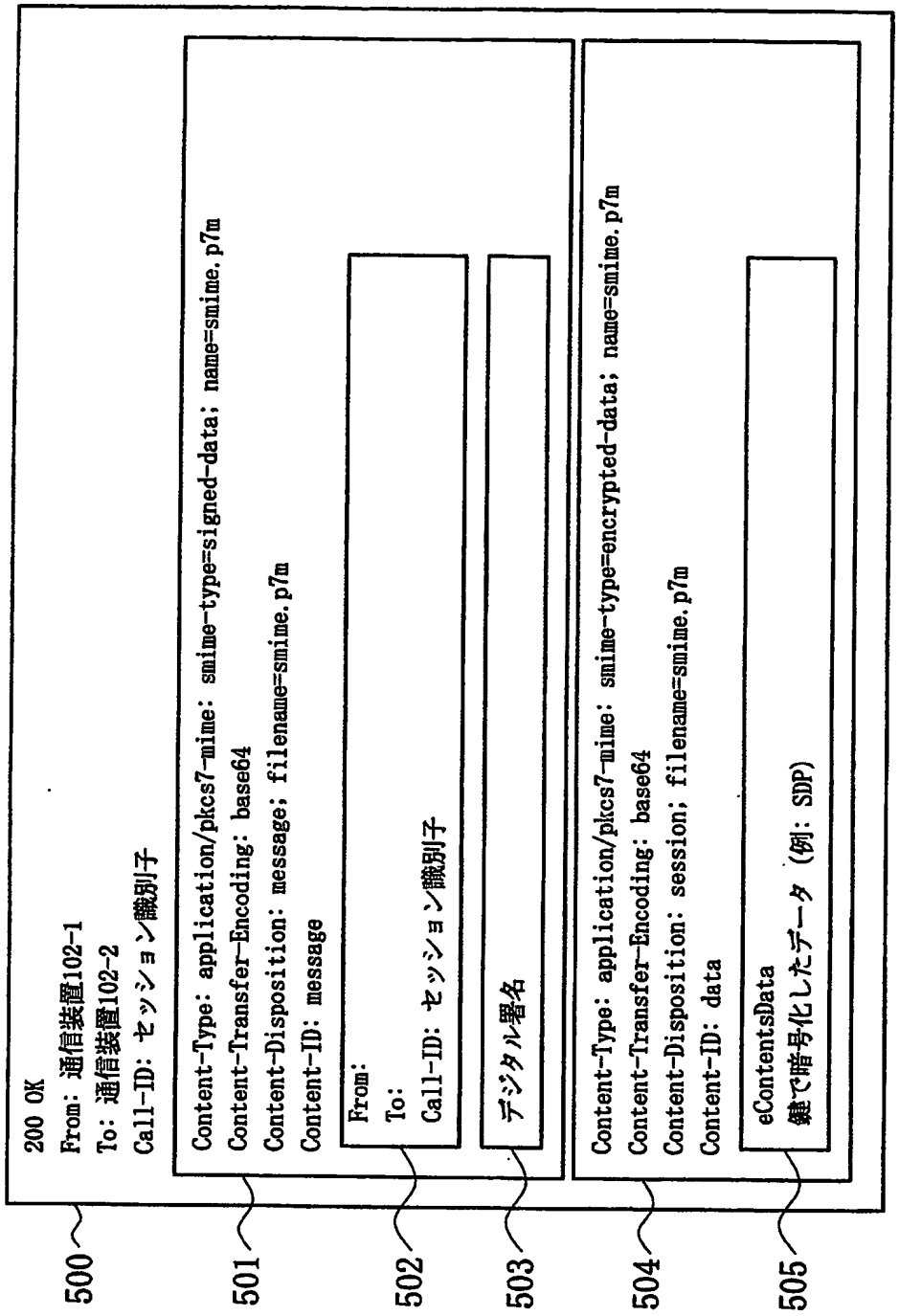
【図３】


10
ネットワーク
102
信号送信手段
120
暗号化鍵生成手段
122
信号暗号化手段
124
信号復号化手段
126
暗号化鍵復号化手段
127
信号受信手段
128
セッション制御手段
121
暗号化鍵暗号化手段
123
暗号化鍵再利用手段
125
暗号化鍵更新手段
129

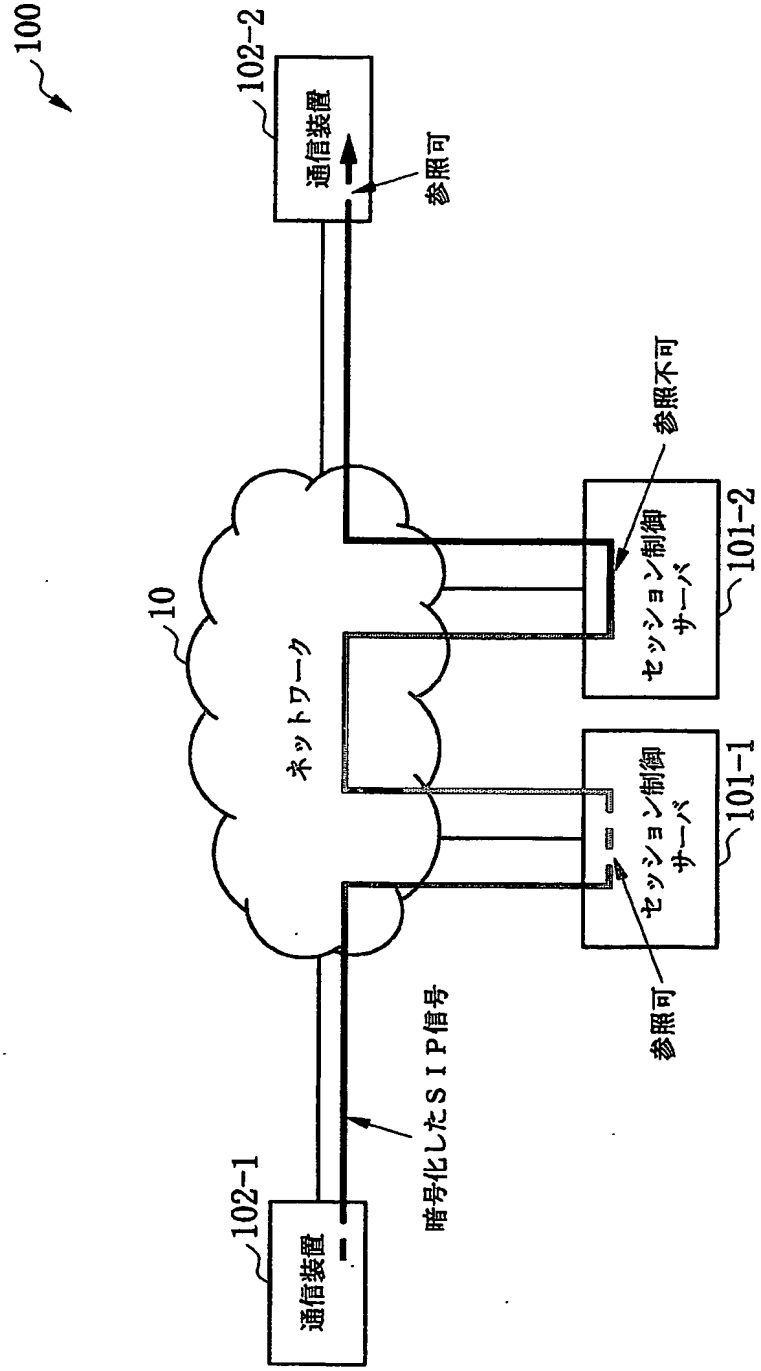
【図４】


INVITE 通信装置102-2 SIP/2.0
From: 通信装置102-1
To: 通信装置102-2
Call-ID: セッション識別子
Content-Type: application/pkcs7-mime; smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: message; filename=smime.p7m
Content-ID: message
From:
To:
Call-ID: セッション識別子
Session-Policy: セッション制御サーバ101; Content-ID: data
デジタル署名
Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: session; filename=smime.p7m
Content-ID: data
eContentsData
鍵で暗号化したデータ (例: SDP)
RecepientInfo
1: 公開鍵: セッション制御サーバ101の鍵識別子: 暗号化した暗号化鍵
2: 公開鍵: 着ユーザの鍵識別子: 暗号化した暗号化鍵
400
401
402
403
404
405
406

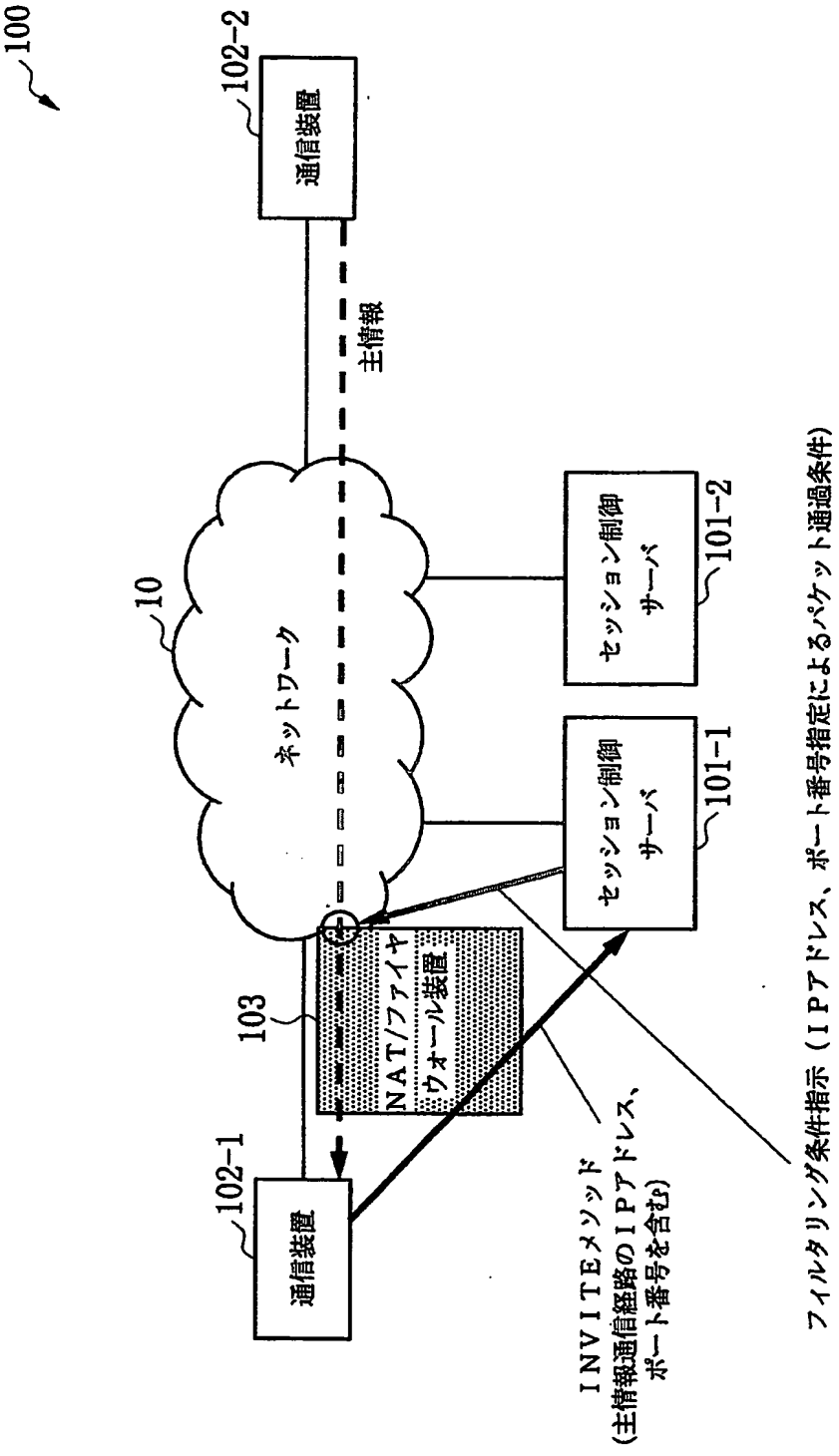
【図５】


200 OK
From: 通信装置102-1
To: 通信装置102-2
Call-ID: セッション識別子
500
Content-Type: application/pkcs7-mime; smime-type=signed-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: message; filename=smime.p7m
Content-ID: message
501
From:
To:
Call-ID: セッション識別子
502
デジタル署名
503
Content-Type: application/pkcs7-mime; smime-type=encrypted-data; name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: session; filename=smime.p7m
Content-ID: data
504
eContentsData
鍵で暗号化したデータ (例: SDP)
505

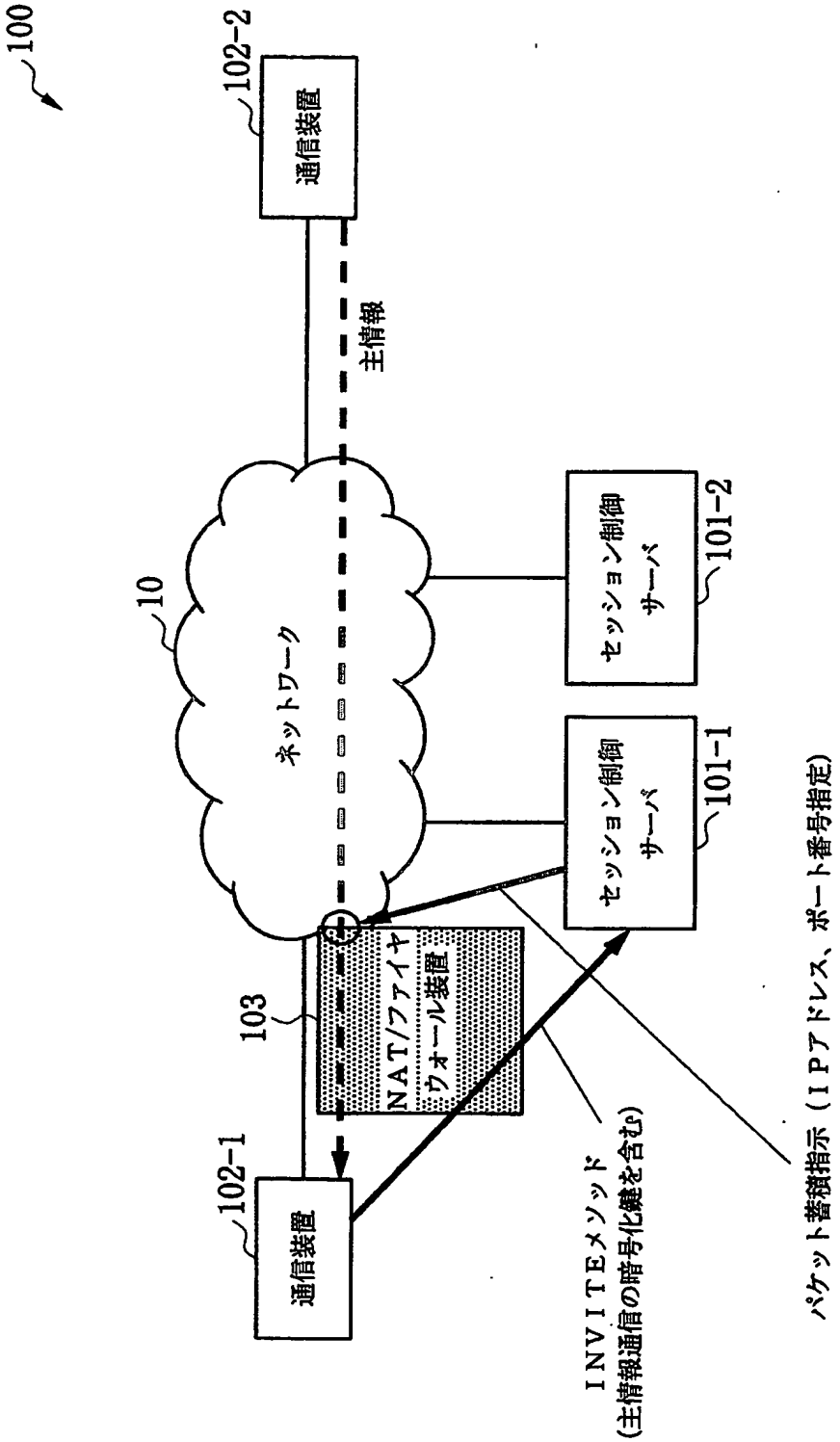
【図６】


100
102-2
通信装置
参照可
参照不可
10
ネットワーク
セッション制御サーバ
101-2
セッション制御サーバ
101-1
参照可
暗号化したＳＩＰ信号
102-1
通信装置

【図７】


100
102-2
通信装置
主情報
10
ネットワーク
セッション制御
サーバ
101-2
セッション制御
サーバ
101-1
103
NAT/ファイヤ
ウォール装置
102-1
通信装置
INVITEメソッド
(主情報通信経路のIPアドレス、
ポート番号を含む)
フィルタリング条件指示（IPアドレス、ポート番号指定によるパケット通過条件）

【図８】


100
102-2
通信装置
主情報
10
ネットワーク
セッション制御
サーバ
101-2
セッション制御
サーバ
101-1
103
NAT/ファイヤ
ウォール装置
102-1
通信装置
INVITEメソッド
(主情報通信の暗号化鍵を含む)
パケット蓄積指示（IPアドレス、ポート番号指定）

【書類名】　　要約書

【要約】

【課題】発着通信端末間の暗号化通信を提供し、かつ特定のセッション制御サーバに対してのみ情報開示を可能とする。

【解決手段】通信装置１０２－１，１０２－２が、情報開示したい特定の中継サーバ１０１－１、または１０１－２の公開鍵で暗号化した情報暗号化鍵を、情報公開鍵で暗号化した情報とともに送信する。また、情報暗号化鍵の暗号化に使用する鍵は、公開鍵の代わりに事前共有鍵も使用可能である。これにより、通信端末で暗号化した情報を選択的にサーバ毎に復号可・不可を制御することが可能となる。

【選択図】　　図１

# 認定・付加情報

| | |
|---|---|
| 特許出願の番号 | 特願２００３－１７６５６８ |
| 受付番号 | ５０３０１０３４１９３ |
| 書類名 | 特許願 |
| 担当官 | 第八担当上席　　００９７ |
| 作成日 | 平成１５年　６月２３日 |

＜認定情報・付加情報＞

【提出日】　平成15年 6月20日

次頁無

# 出願人履歴情報

識別番号　[０００００４２２６]

１．変更年月日　１９９９年　７月１５日
[変更理由]　住所変更
住　所　東京都千代田区大手町二丁目３番１号
氏　名　日本電信電話株式会社